Cyber Risk Responsibilities

Identifying Cyber Threats

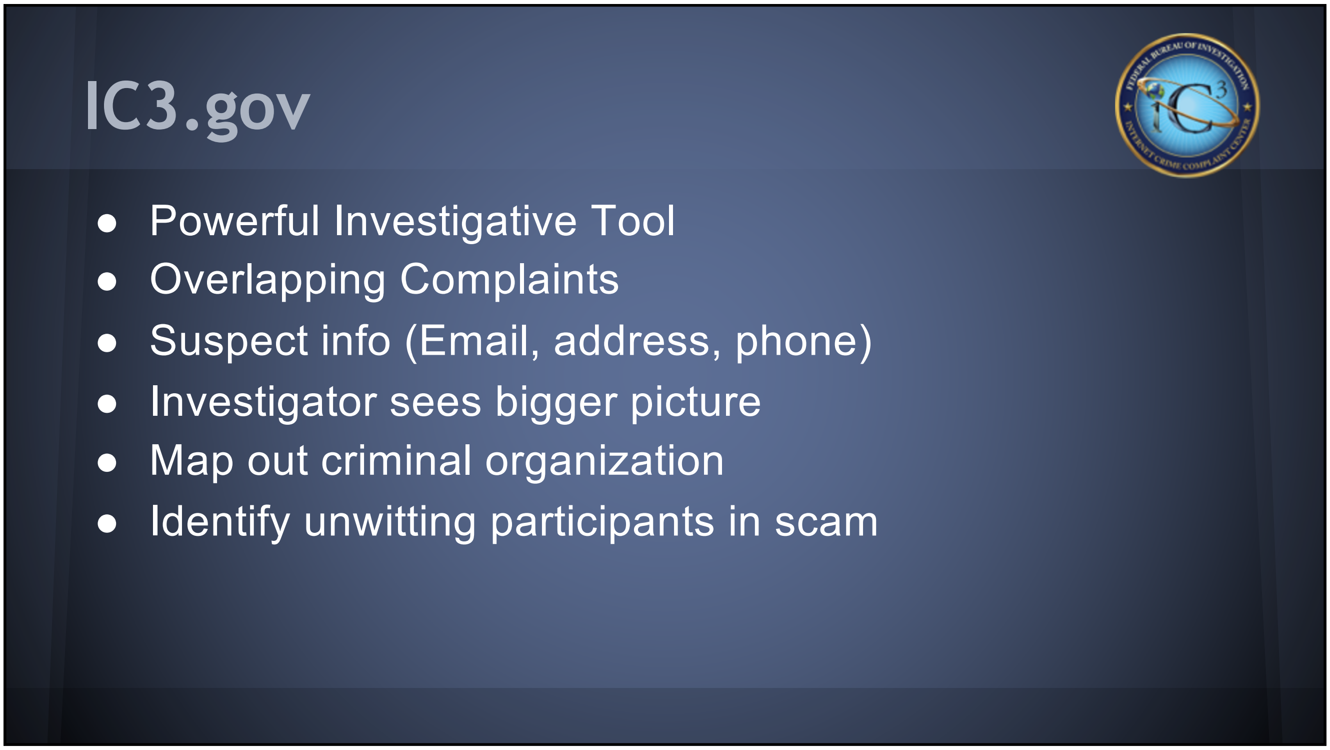
Sgt. Jeffrey Plank

1

Operation Wellspring

- Established in July 2013
- Is a collaboration between FBI Special Agents and Agents from the Department of Public Safety/State Bureau of Investigation.
- Agents are housed with the FBI and have access to their data bases.
- Agents investigate various kinds of Internet fraud and computer intrusions which are reported through the Internet Crimes Complaint Center (IC3.gov).

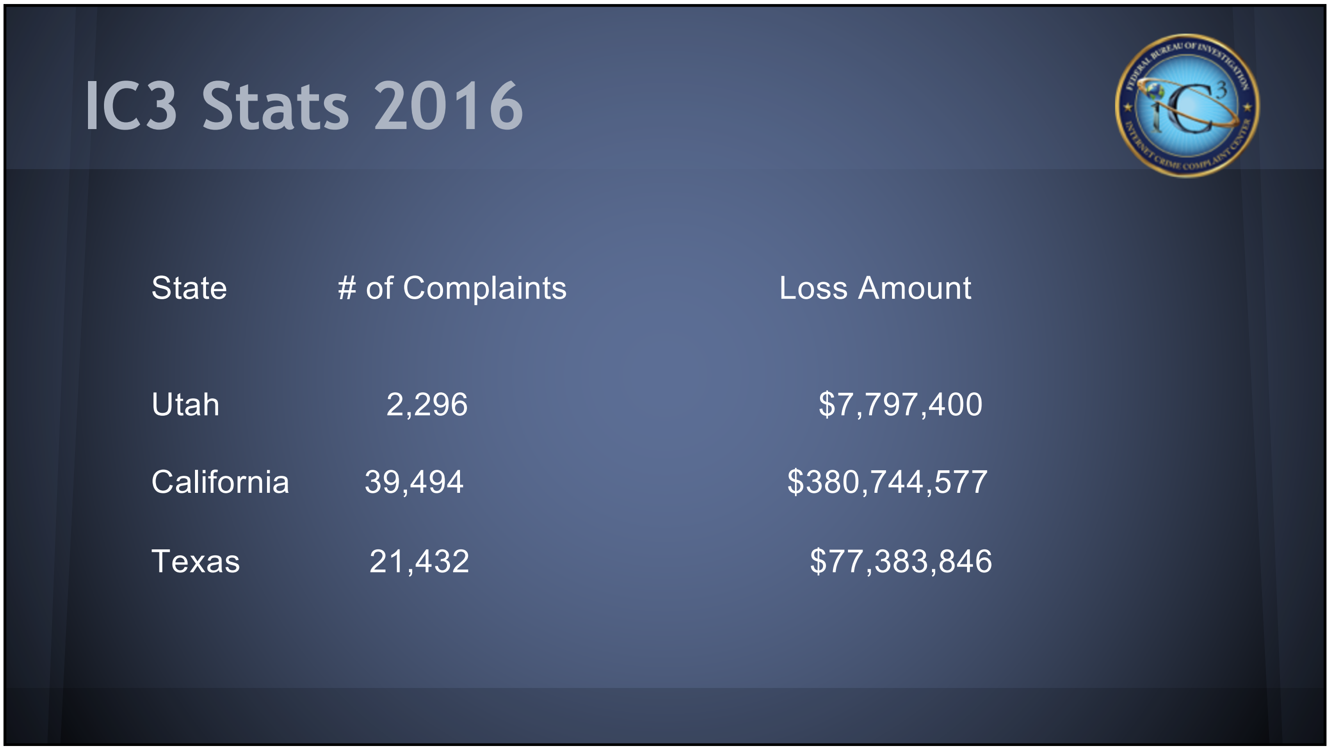
2



IC3.gov

- Powerful Investigative Tool
- Overlapping Complaints
- Suspect info (Email, address, phone)
- Investigator sees bigger picture
- Map out criminal organization
- Identify unwitting participants in scam

3

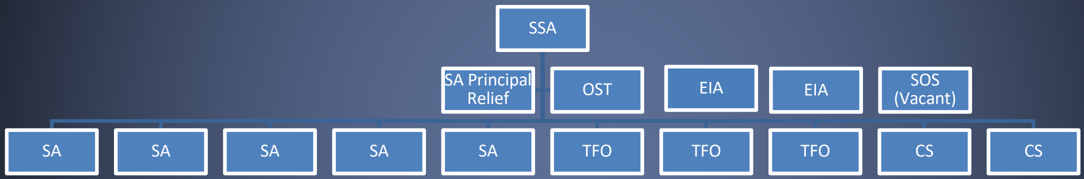


IC3 Stats 2016

State	# of Complaints	Loss Amount
Utah	2,296	$7,797,400
California	39,494	$380,744,577
Texas	21,432	$77,383,846

4

FBI Salt Lake City Cyber Task Force



SSA

SA Principal Relief

OST

EIA

EIA

SOS (Vacant)

SA

SA

SA

SA

SA

TFO

TFO

TFO

CS

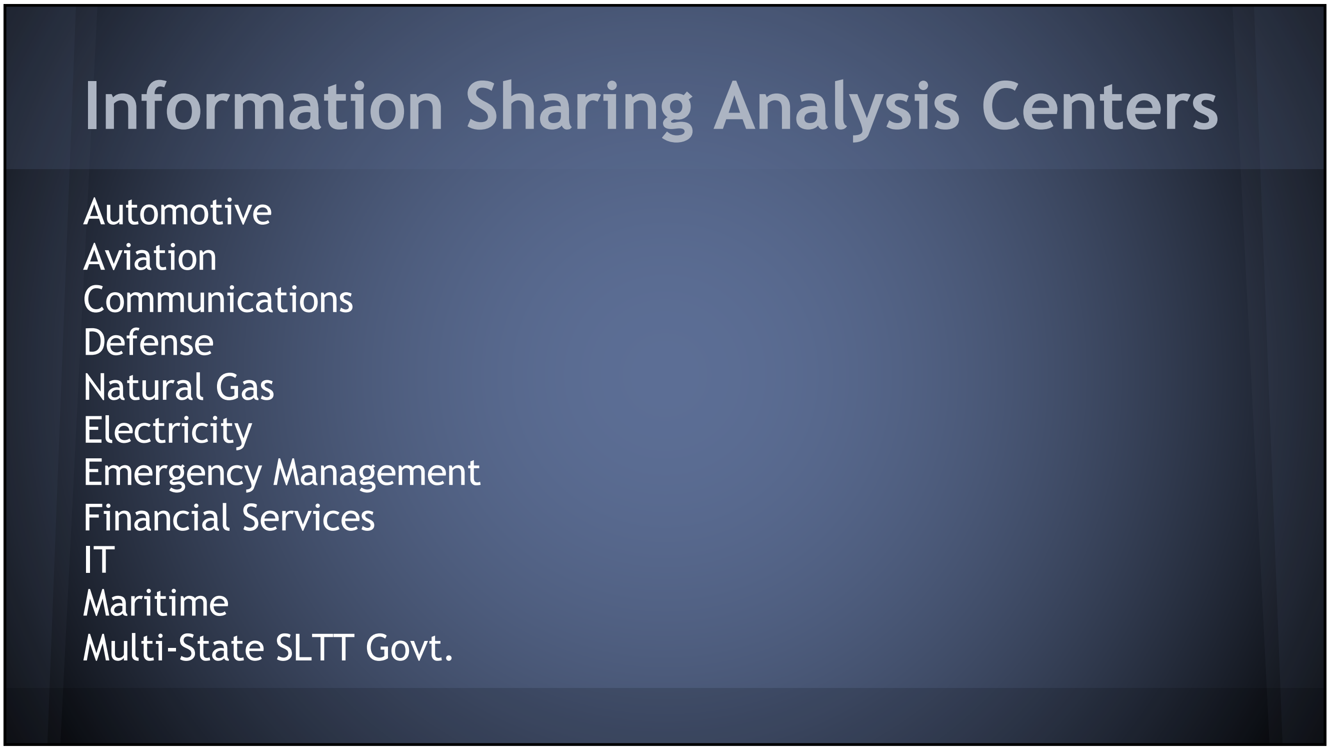
CS

SSA	Supervisory Special Agent
SA	Special Agent
TFO	Task Force Officer
EIA	Embedded Intelligence Analyst
CS	Computer Scientist
OST	Operational Support Technician
SOS	Staff Operation Specialist

5

How do we tackle cybercrime?

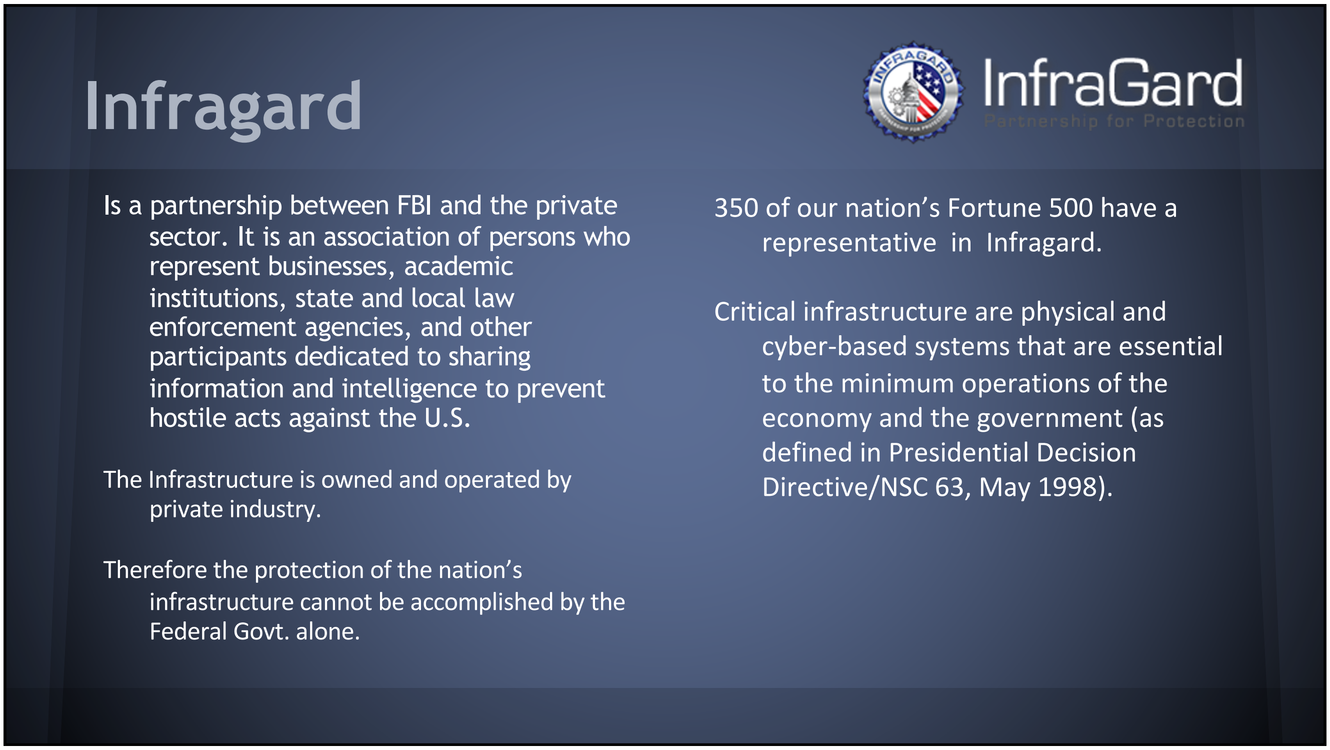
6



Information Sharing Analysis Centers

Automotive
Aviation
Communications
Defense
Natural Gas
Electricity
Emergency Management
Financial Services
IT
Maritime
Multi-State SLTT Govt.

7



Infragard

InfraGard
Partnership for Protection

Is a partnership between FBI and the private sector. It is an association of persons who represent businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the U.S.

The Infrastructure is owned and operated by private industry.

Therefore the protection of the nation's infrastructure cannot be accomplished by the Federal Govt. alone.

350 of our nation's Fortune 500 have a representative in Infragard.

Critical infrastructure are physical and cyber-based systems that are essential to the minimum operations of the economy and the government (as defined in Presidential Decision Directive/NSC 63, May 1998).

8

16 Critical Infrastructure Sectors

Chemical
Financial
Commercial Facilities
Food and Agriculture
Communications
Govt. Facilities
Healthcare and Public health

Dams
Information Technology
Defense Industrial Base
Nuclear Reactors, Materials and Waste
Emergency Services
Transportation Systems
Energy

9

Infragard Portal

Infragard.org

USE YOUR INFRAGARD ACCOUNT TO LOGIN

InfraGard
Partnership for Protection

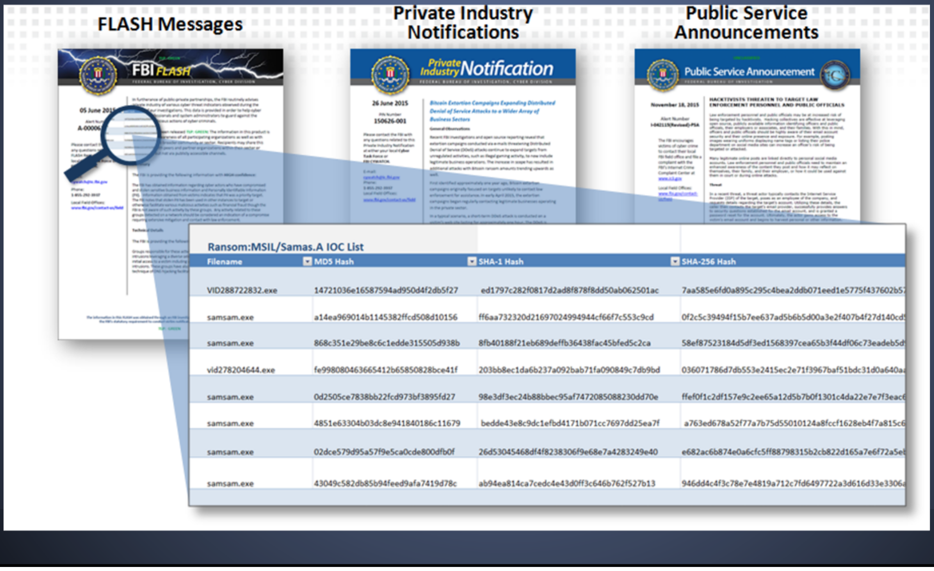
User Name
Password
Forgot Password

New InfraGard Portal

Welcome to new InfraGard portal, join and explore our new features.

10

FBI Information Sharing


FLASH Messages
Private Industry Notifications
Public Service Announcements
FBI FLASH
Private Industry Notification
Public Service Announcement

Ransom:MSIL/Samas.A IOC List

Filename	MD5 Hash	SHA-1 Hash	SHA-256 Hash
VID288722832.exe	14721036e16587594ad950d4f2db5f27	ed1797c282f0817d2ad8f878f8dd50ab062501ac	7aa585e6fd0a895c295c4bea2ddb071eed1e5775f437602b5
samsam.exe	a14ea969014b1145382ffcd508d10156	ff6aa732320d21697024994944cf66f7c553c9cd	0f2c5c39494f15b7ee637ad5b6b5d00a3e2f407b4f27d140cd
samsam.exe	868c351e29be8c6c1edde315505d938b	8fb40188f21eb689deffb36438fac45bfed5c2ca	58ef87523184d5df3ed1568397cea65b3f44df06c73eadeb5d
vid278204644.exe	fe998080463665412b65850828bce41f	203bb8ec1da6b237a092bab71fa090849c7db9bd	036071786d7db553e2415ec2e71f3967baf51bdc31d0a640a
samsam.exe	0d2505ce7838bb22fcd973bf3895fd27	98e3df3ec24b88bbec95af7472085088230dd70e	ffef0f1c2df157e9c2ee65a12d5b7b0f1301c4da22e7e7f3eac
samsam.exe	4851e63304b03dc8e941840186c11679	bedde43e8c9dc1efbd4171b071cc7697dd25ea7f	a763ed678a52f77a7b75d55010124a8fccf1628eb4f7a815c6
samsam.exe	02dce579d95a57f9e5ca0cde800dfb0f	26d53045468df4f8238306f9e68e7a4283249e40	e682ac6b874e0a6cfc5ff88798315b2cb822d165a7e6f72a5e
samsam.exe	43049c582db85b94feed9afa7419d78c	ab94ea814ca7cedc4e43d0ff3c646b762f527b13	946dd4c4f3c78e7e4819a712c7fd6497722a3d616d33e3306

11

Title 18 U.S.C 1030

- Computer Fraud and Abuse Act (CFAA)
  - Outlaws conduct that victimizes computer systems.
  - Cyber security law.
  - Protects federal computers, bank computers, and computers connected to the Internet.
  - Shields them from trespassing, threats, damage, espionage, and from being corruptly used as instruments of Fraud.

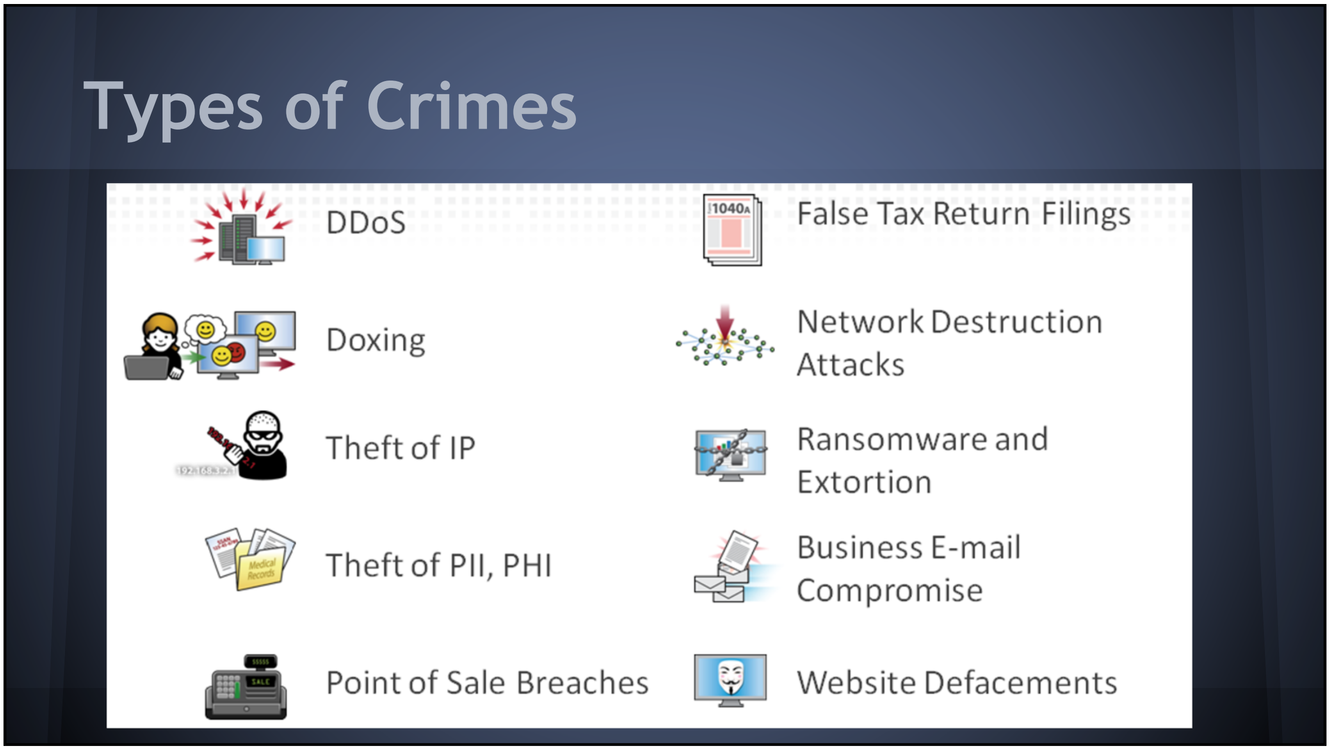
12

76-6-703

- Computer Crimes and Penalties
  - A person who without authorization gains or attempts to gain access to and alters, damages, destroys, discloses, or modifies any computer, computer network, computer property, computer system, computer program, computer data or software, and thereby causes damage to another, or obtains money, property, information, or a benefit for any person without legal right.

13

14

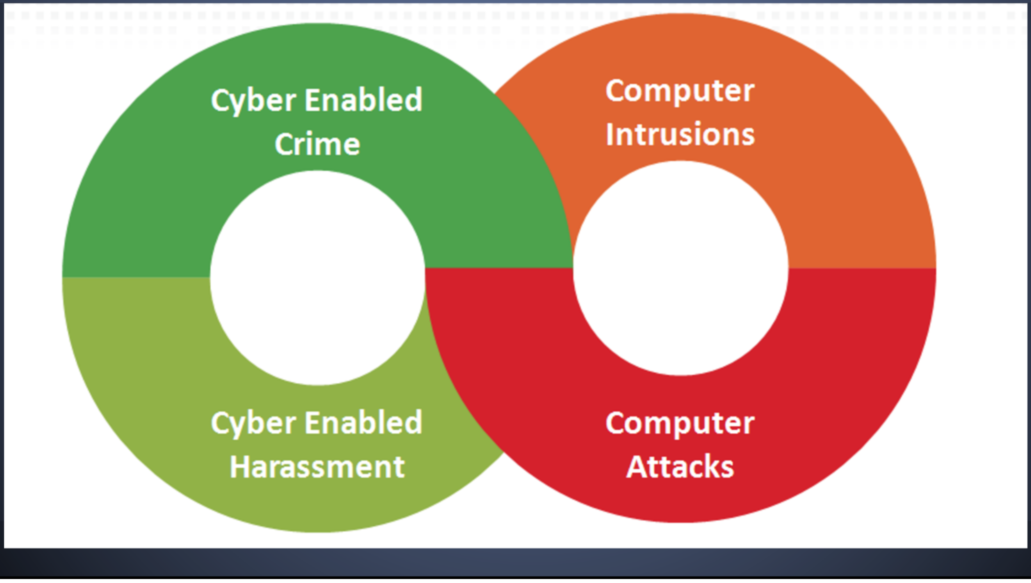


Types of Crimes

- DDoS
- Doxing
- Theft of IP
- Theft of PII, PHI
- Point of Sale Breaches
- False Tax Return Filings
- Network Destruction Attacks
- Ransomware and Extortion
- Business E-mail Compromise
- Website Defacements

15

Cyber Enabled vs. Computer Crime



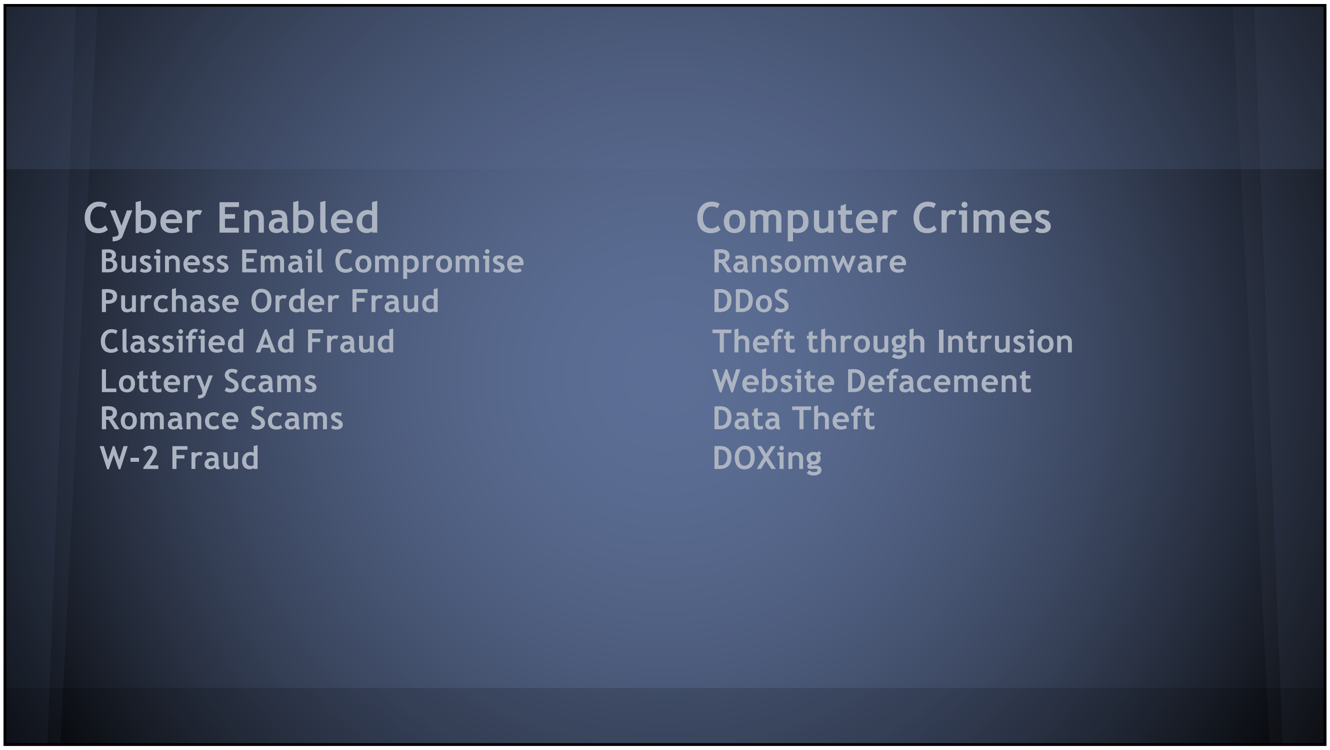
Cyber Enabled Crime

Computer Intrusions

Cyber Enabled Harassment

Computer Attacks

16



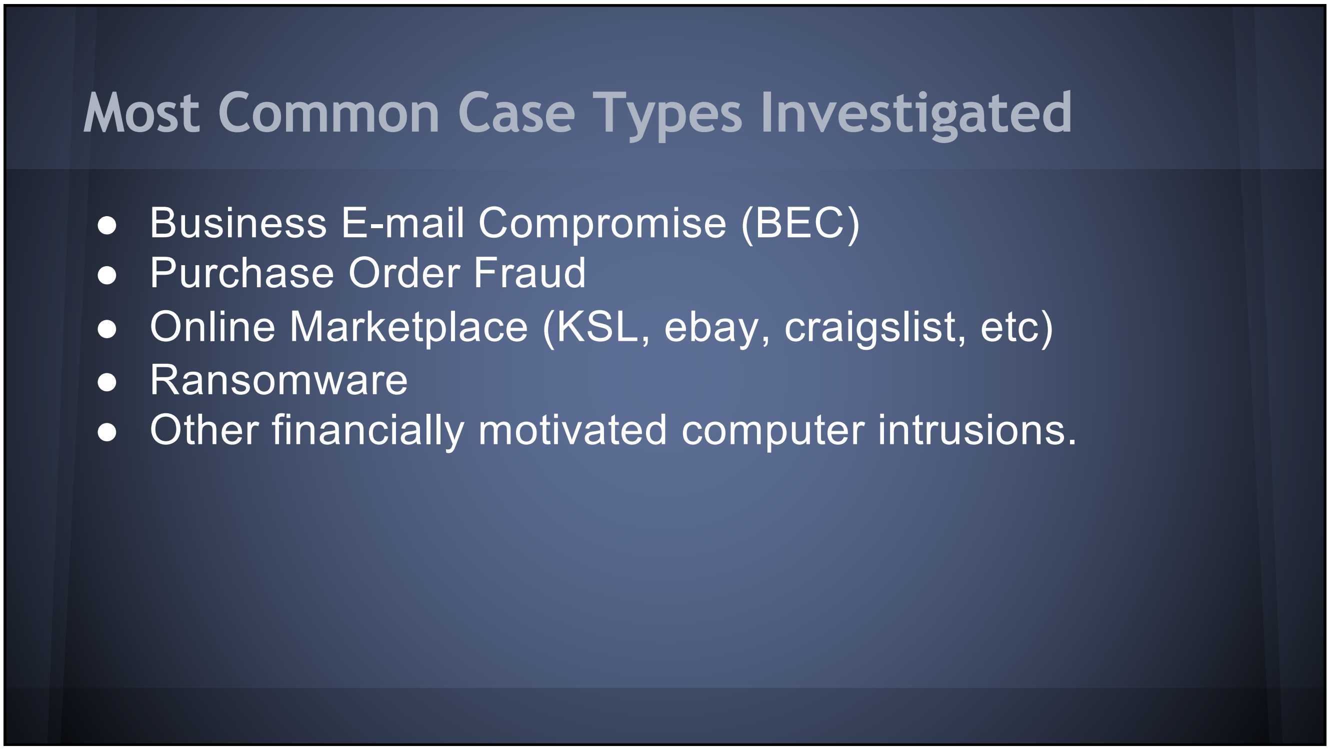
Cyber Enabled

- Business Email Compromise
- Purchase Order Fraud
- Classified Ad Fraud
- Lottery Scams
- Romance Scams
- W-2 Fraud

Computer Crimes

- Ransomware
- DDoS
- Theft through Intrusion
- Website Defacement
- Data Theft
- DOXing

17

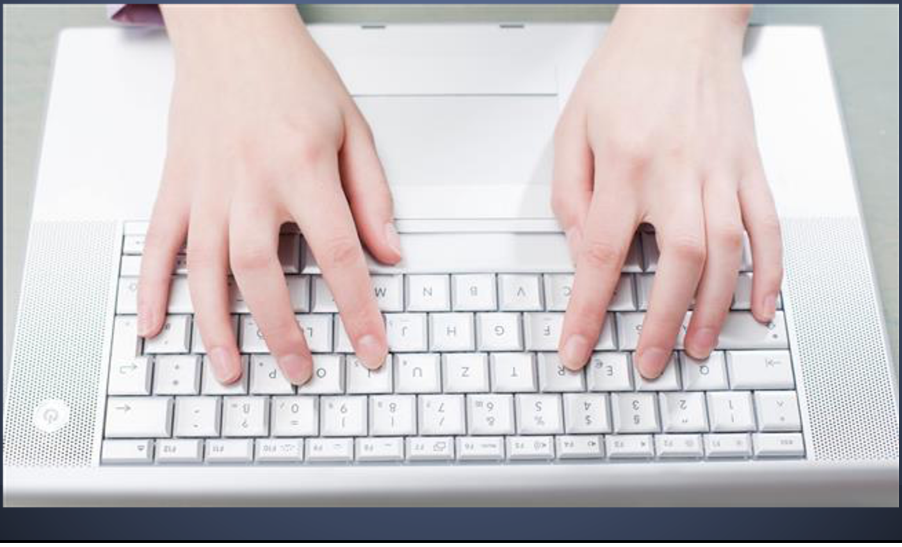


Most Common Case Types Investigated

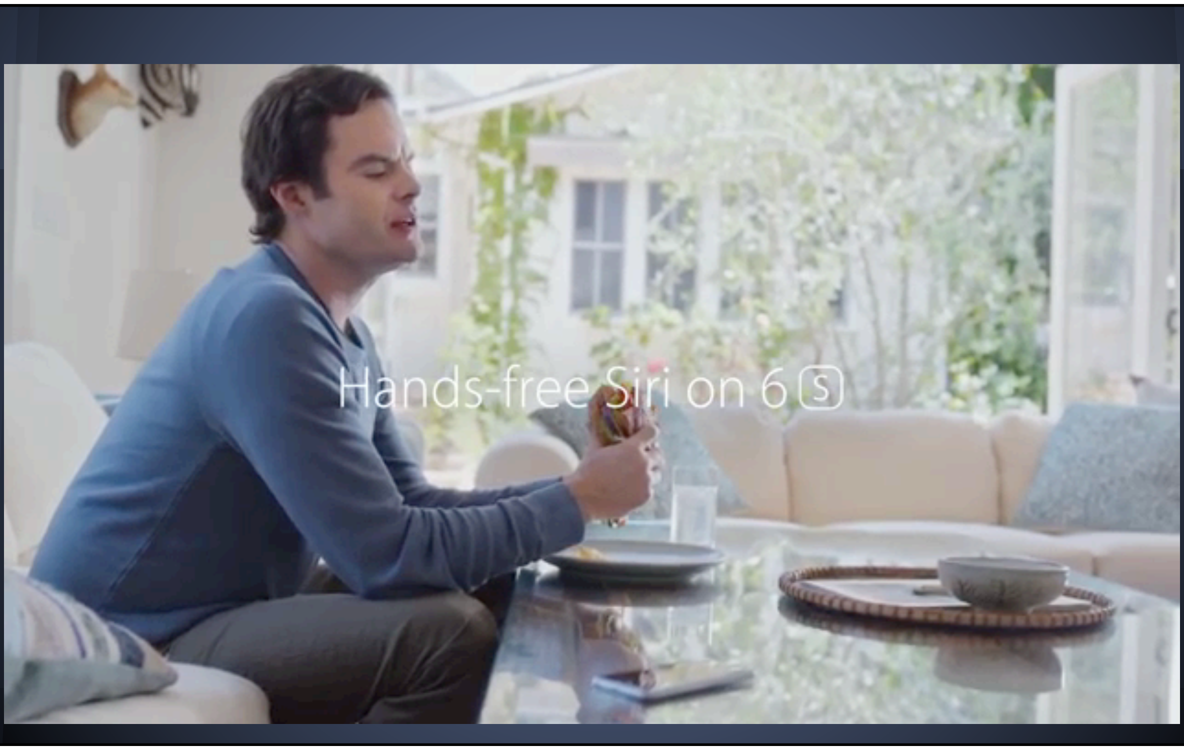
- Business E-mail Compromise (BEC)
- Purchase Order Fraud
- Online Marketplace (KSL, ebay, craigslist, etc)
- Ransomware
- Other financially motivated computer intrusions.

18

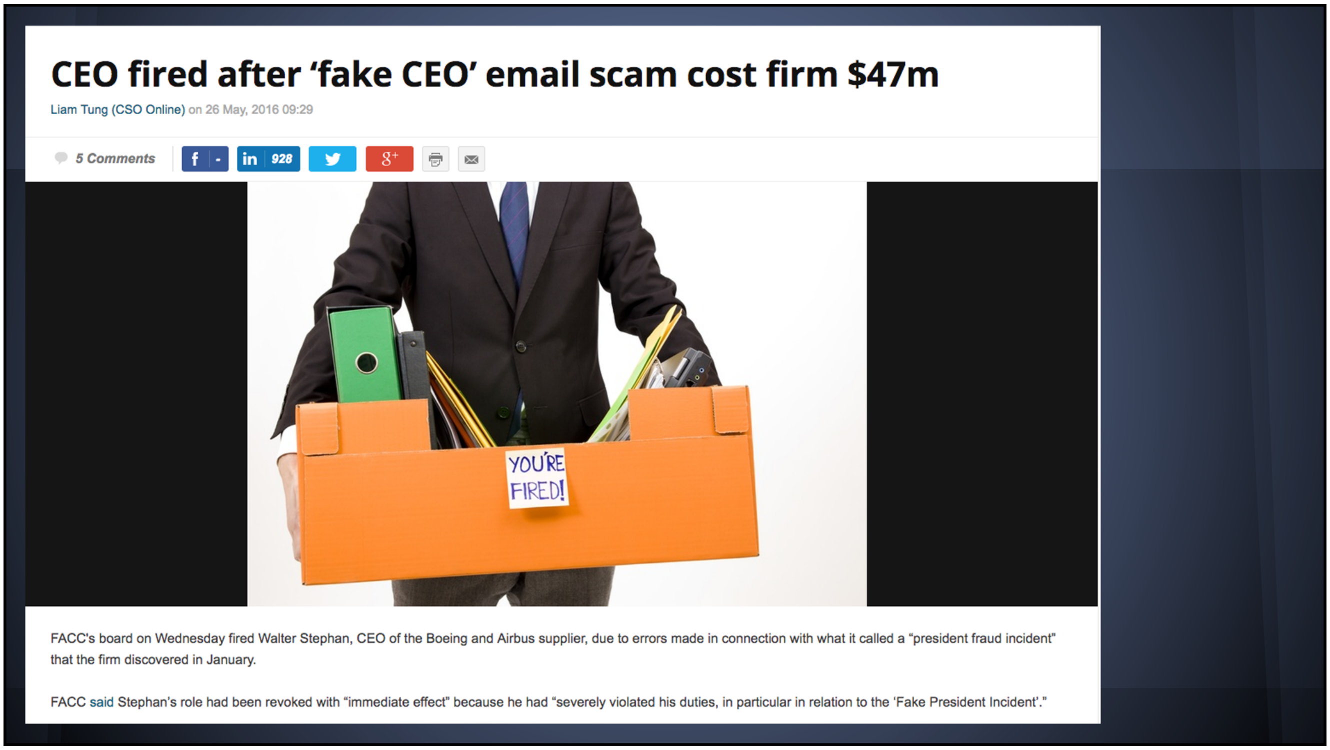
Cyber Enabled



19



20



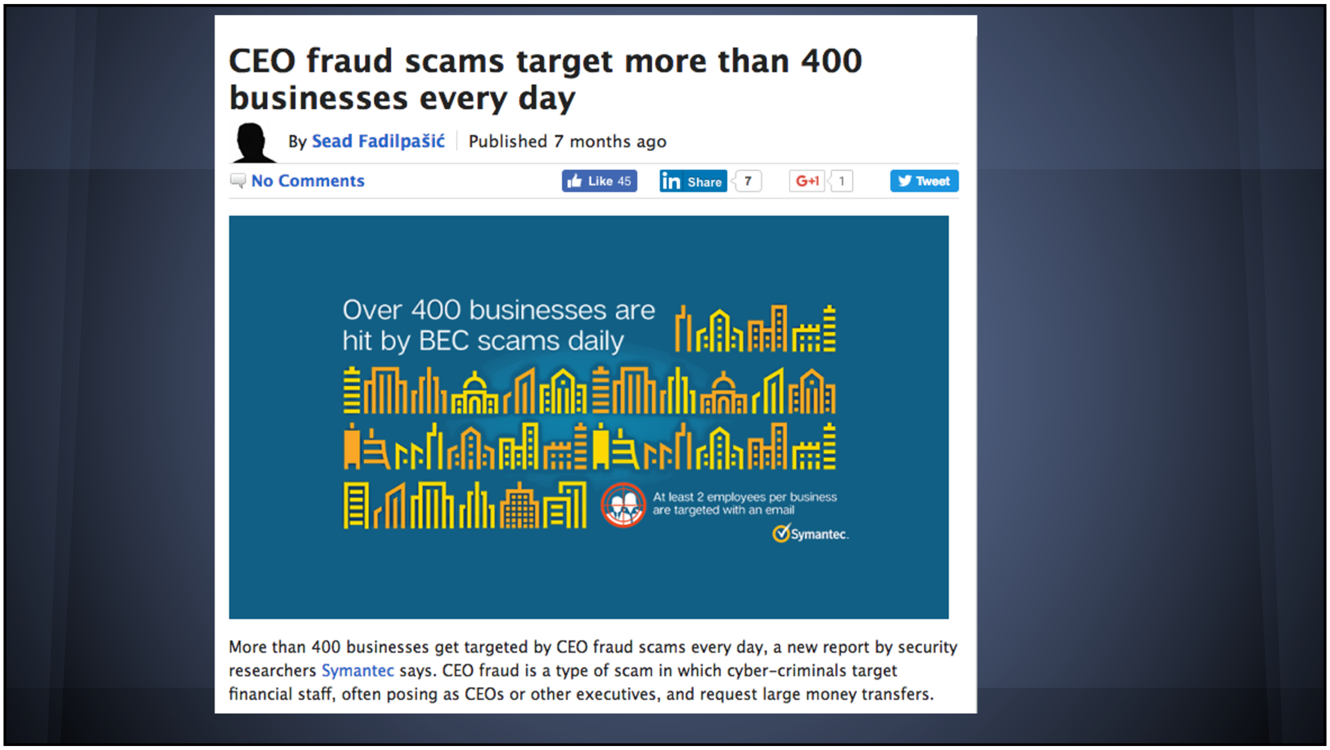
CEO fired after 'fake CEO' email scam cost firm $47m

Liam Tung (CSO Online) on 26 May, 2016 09:29

FACC's board on Wednesday fired Walter Stephan, CEO of the Boeing and Airbus supplier, due to errors made in connection with what it called a "president fraud incident" that the firm discovered in January.

FACC said Stephan's role had been revoked with "immediate effect" because he had "severely violated his duties, in particular in relation to the 'Fake President Incident'."

21

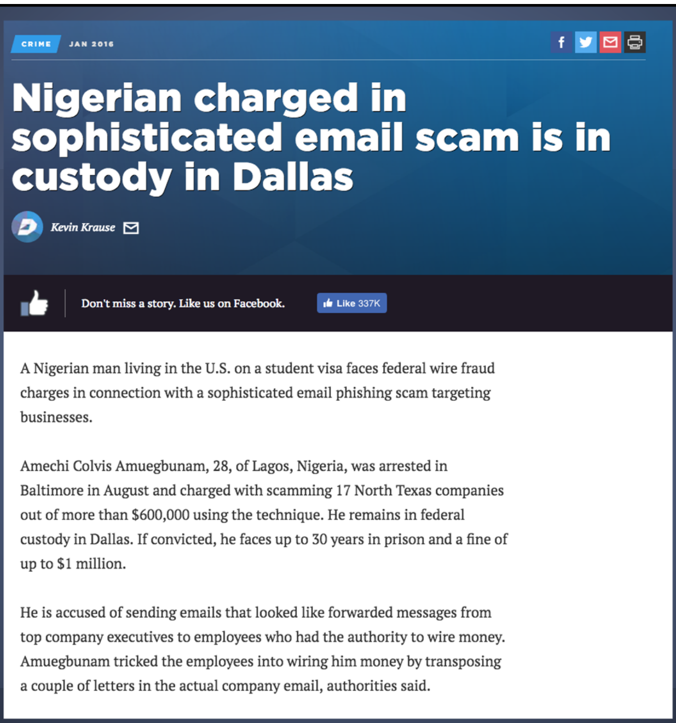


CEO fraud scams target more than 400 businesses every day

By Sead Fadilpašić | Published 7 months ago

More than 400 businesses get targeted by CEO fraud scams every day, a new report by security researchers Symantec says. CEO fraud is a type of scam in which cyber-criminals target financial staff, often posing as CEOs or other executives, and request large money transfers.

22



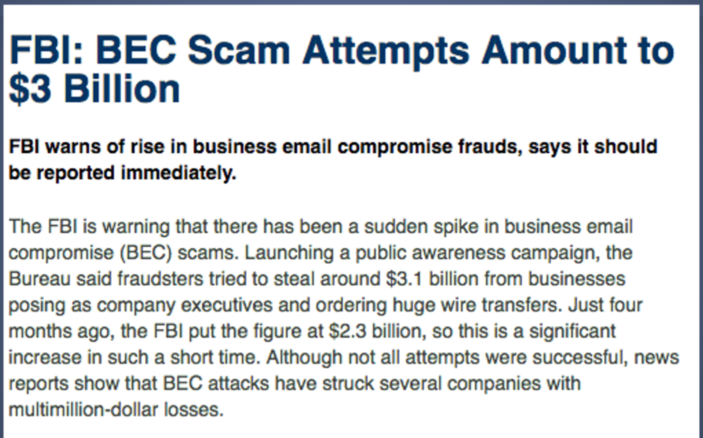
Nigerian charged in sophisticated email scam is in custody in Dallas

A Nigerian man living in the U.S. on a student visa faces federal wire fraud charges in connection with a sophisticated email phishing scam targeting businesses.

Amechi Colvis Amuegbunam, 28, of Lagos, Nigeria, was arrested in Baltimore in August and charged with scamming 17 North Texas companies out of more than $600,000 using the technique. He remains in federal custody in Dallas. If convicted, he faces up to 30 years in prison and a fine of up to $1 million.

He is accused of sending emails that looked like forwarded messages from top company executives to employees who had the authority to wire money. Amuegbunam tricked the employees into wiring him money by transposing a couple of letters in the actual company email, authorities said.

23



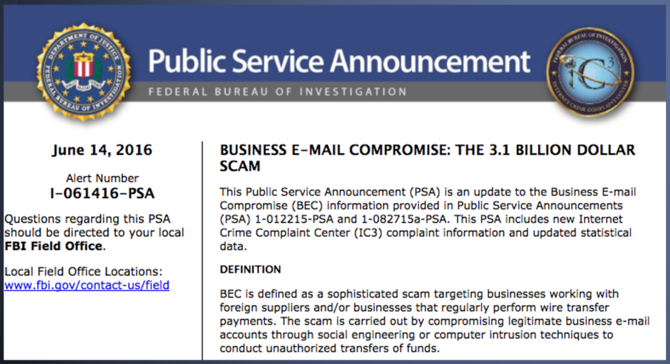
FBI: BEC Scam Attempts Amount to $3 Billion

FBI warns of rise in business email compromise frauds, says it should be reported immediately.

The FBI is warning that there has been a sudden spike in business email compromise (BEC) scams. Launching a public awareness campaign, the Bureau said fraudsters tried to steal around $3.1 billion from businesses posing as company executives and ordering huge wire transfers. Just four months ago, the FBI put the figure at $2.3 billion, so this is a significant increase in such a short time. Although not all attempts were successful, news reports show that BEC attacks have struck several companies with multimillion-dollar losses.

24

Business Email Compromise PSA



June 14, 2016

Alert Number
I-061416-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

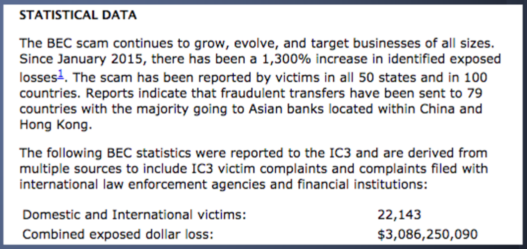
Local Field Office Locations: www.fbi.gov/contact-us/field

BUSINESS E-MAIL COMPROMISE: THE 3.1 BILLION DOLLAR SCAM

This Public Service Announcement (PSA) is an update to the Business E-mail Compromise (BEC) information provided in Public Service Announcements (PSA) 1-012215-PSA and 1-082715a-PSA. This PSA includes new Internet Crime Complaint Center (IC3) complaint information and updated statistical data.

DEFINITION

BEC is defined as a sophisticated scam targeting businesses working with foreign suppliers and/or businesses that regularly perform wire transfer payments. The scam is carried out by compromising legitimate business e-mail accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds.



STATISTICAL DATA

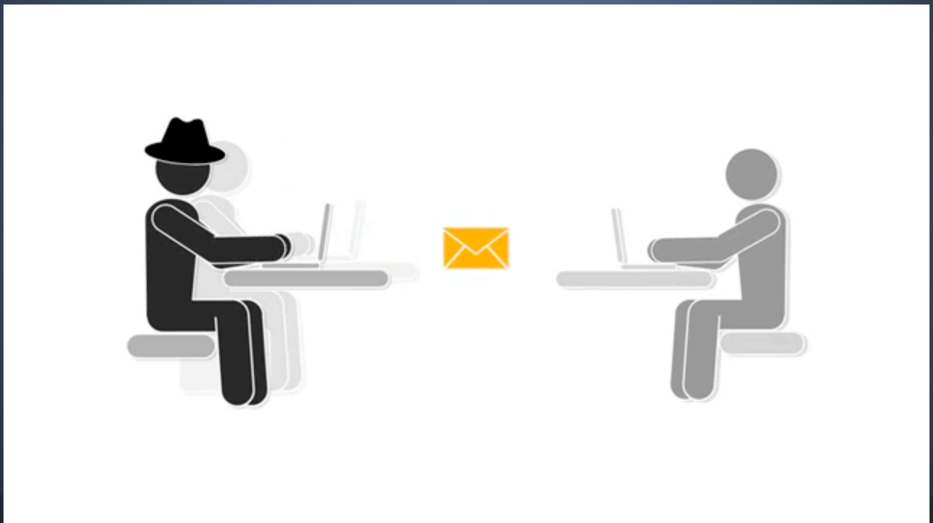
The BEC scam continues to grow, evolve, and target businesses of all sizes. Since January 2015, there has been a 1,300% increase in identified exposed losses[1]. The scam has been reported by victims in all 50 states and in 100 countries. Reports indicate that fraudulent transfers have been sent to 79 countries with the majority going to Asian banks located within China and Hong Kong.

The following BEC statistics were reported to the IC3 and are derived from multiple sources to include IC3 victim complaints and complaints filed with international law enforcement agencies and financial institutions:

Domestic and International victims:	22,143
Combined exposed dollar loss:	$3,086,250,090

25

Business Email Compromise



26

How it works.

Suspect identifies a target. Obtains information from email account that helps them social engineer the victim. (Signature, forms, vacation, etc.)

Obtains a website domain that is similar to target-normally the same day or day before the wire transfer.

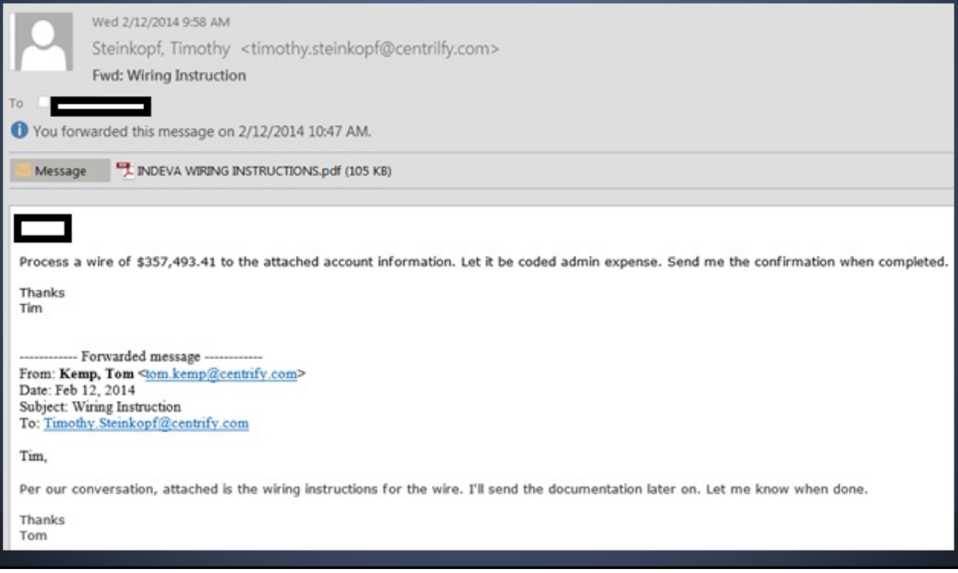
Example.com can be changed to look like:

- Example.net or .org, etc.
- Examp1e.net or .org, etc.
- Exanple.net or .org, etc.

james@examp1e.net sends the email and impersonates the CEO.

27

BEC



Wed 2/12/2014 9:58 AM
Steinkopf, Timothy <timothy.steinkopf@centrilfy.com>
Fwd: Wiring Instruction

To [redacted]

You forwarded this message on 2/12/2014 10:47 AM.

Message | INDEVA WIRING INSTRUCTIONS.pdf (105 KB)

[redacted]

Process a wire of $357,493.41 to the attached account information. Let it be coded admin expense. Send me the confirmation when completed.

Thanks
Tim

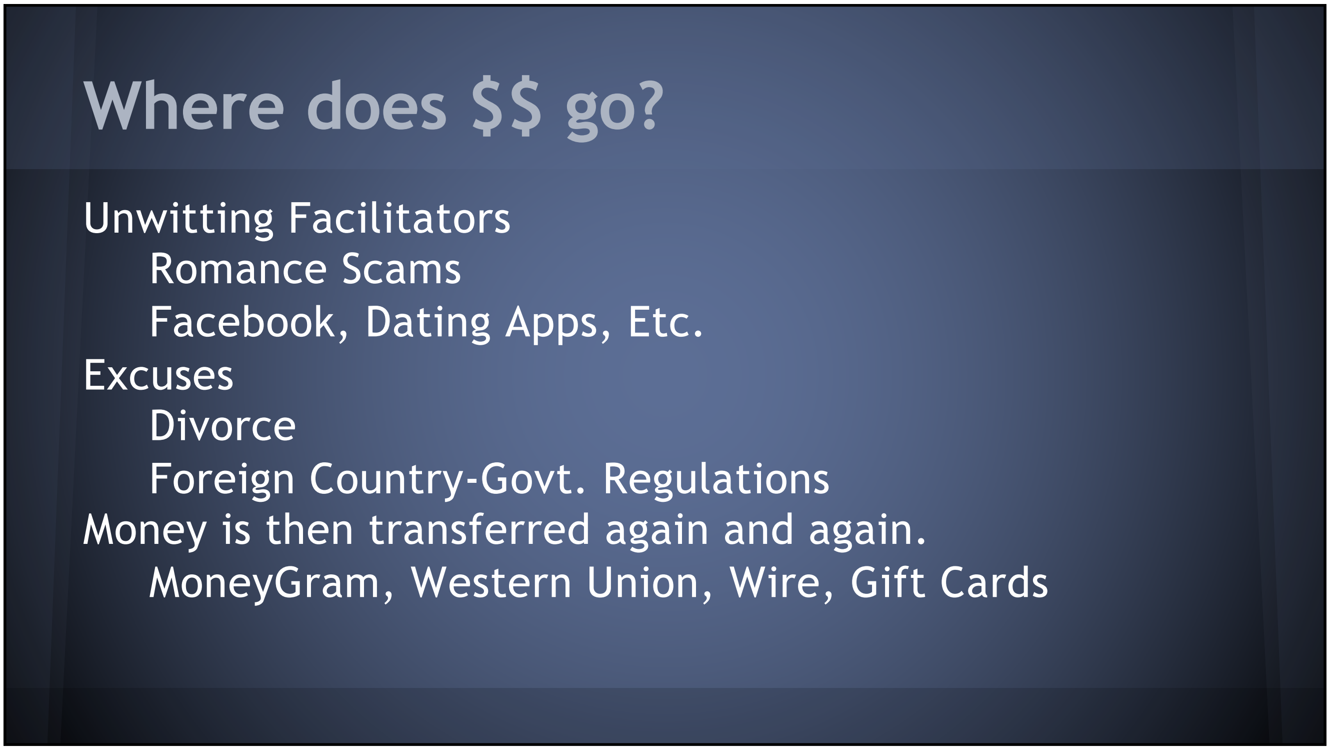
------------ Forwarded message ------------
From: **Kemp, Tom** <tom.kemp@centrify.com>
Date: Feb 12, 2014
Subject: Wiring Instruction
To: Timothy.Steinkopf@centrify.com

Tim,

Per our conversation, attached is the wiring instructions for the wire. I'll send the documentation later on. Let me know when done.

Thanks
Tom

28



Where does $$ go?

Unwitting Facilitators

- Romance Scams
- Facebook, Dating Apps, Etc.

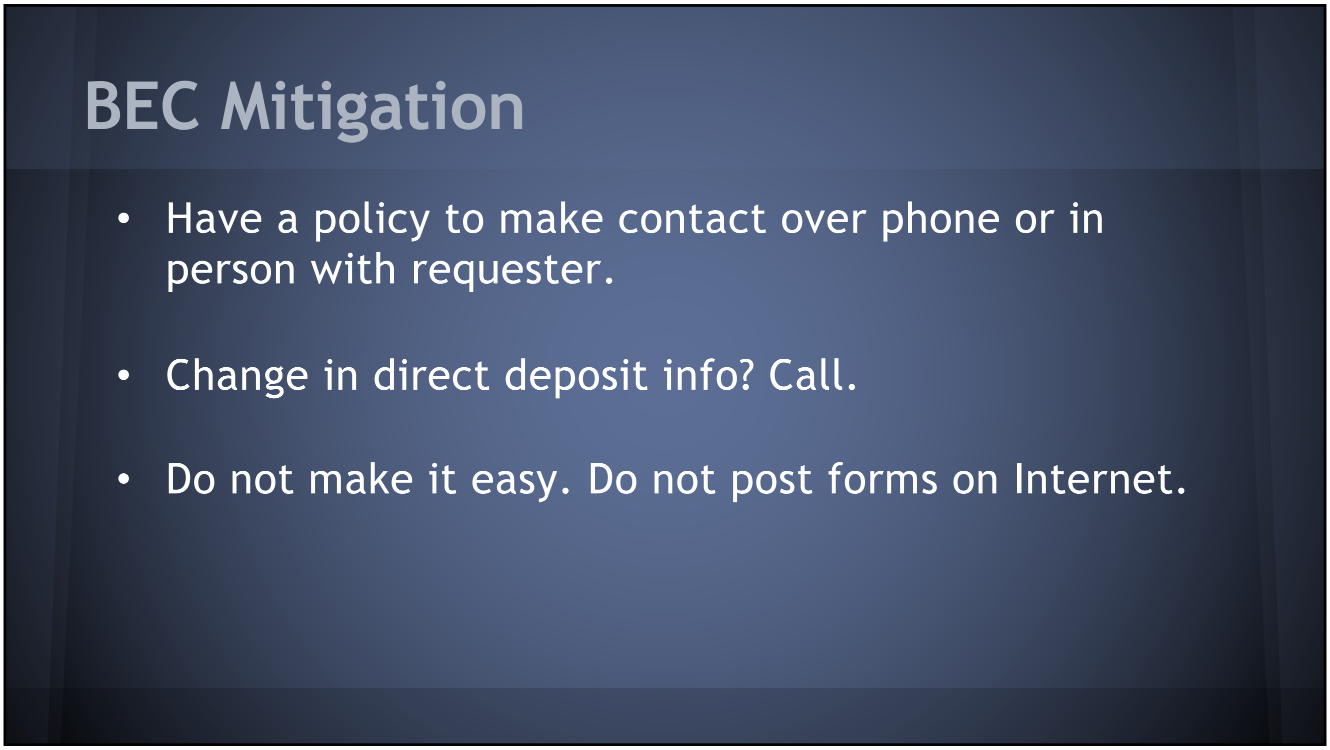
Excuses

- Divorce
- Foreign Country-Govt. Regulations

Money is then transferred again and again.

- MoneyGram, Western Union, Wire, Gift Cards

29



BEC Mitigation

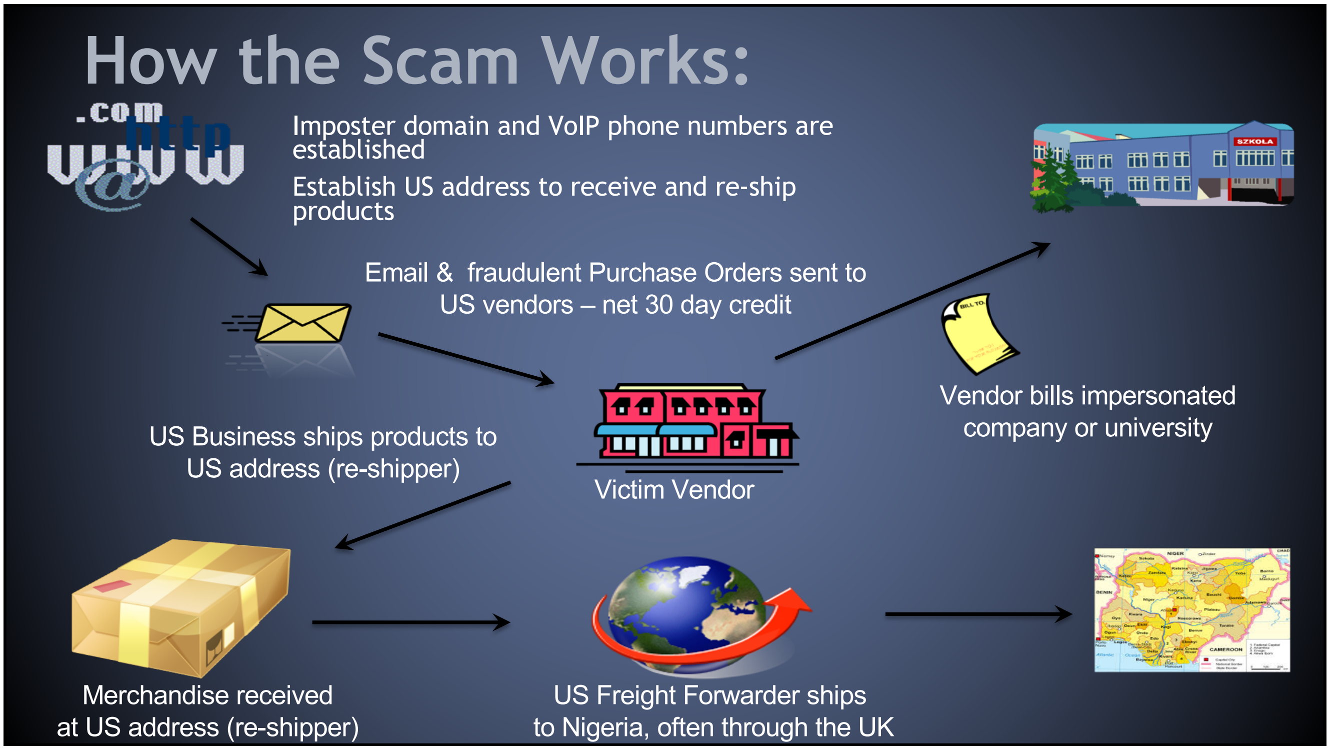
- Have a policy to make contact over phone or in person with requester.
- Change in direct deposit info? Call.
- Do not make it easy. Do not post forms on Internet.

30

PO Fraud

- University or corporate identities are impersonated to obtain merchandise on credit.
- Merchandise is shipped before the victim vendor discovers the fraud.
- Scammers operate primarily from Nigeria or outside of U.S. Jurisdiction.

31



How the Scam Works:

Imposter domain and VoIP phone numbers are established

Establish US address to receive and re-ship products

Email & fraudulent Purchase Orders sent to US vendors – net 30 day credit

Vendor bills impersonated company or university

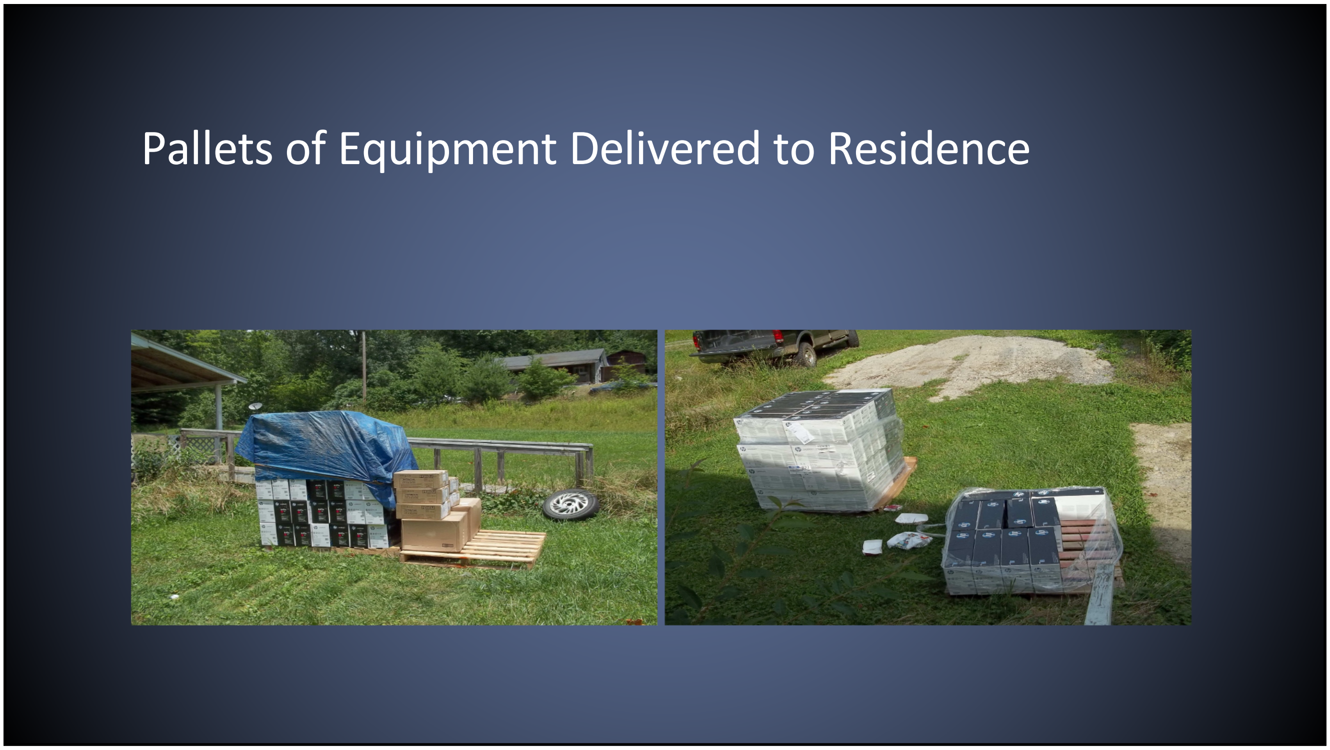
US Business ships products to US address (re-shipper)

Victim Vendor

Merchandise received at US address (re-shipper)

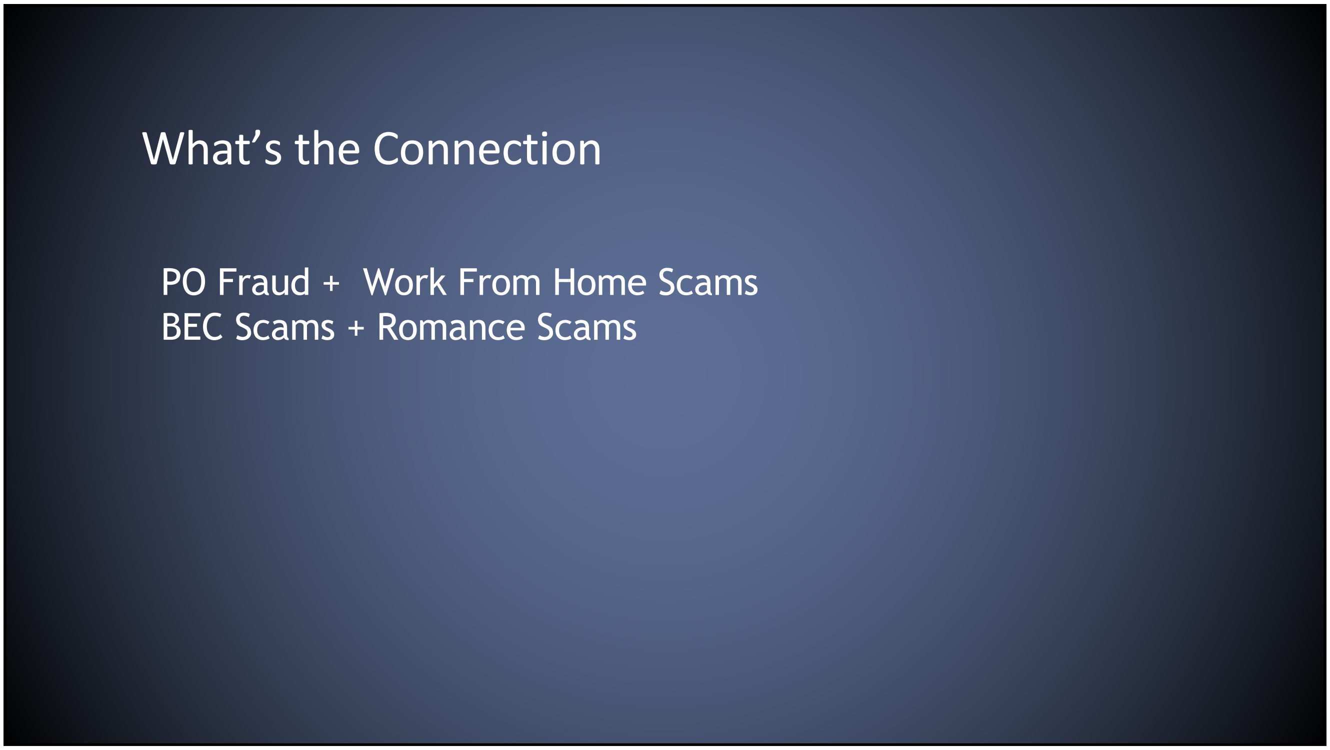
US Freight Forwarder ships to Nigeria, often through the UK

32



Pallets of Equipment Delivered to Residence

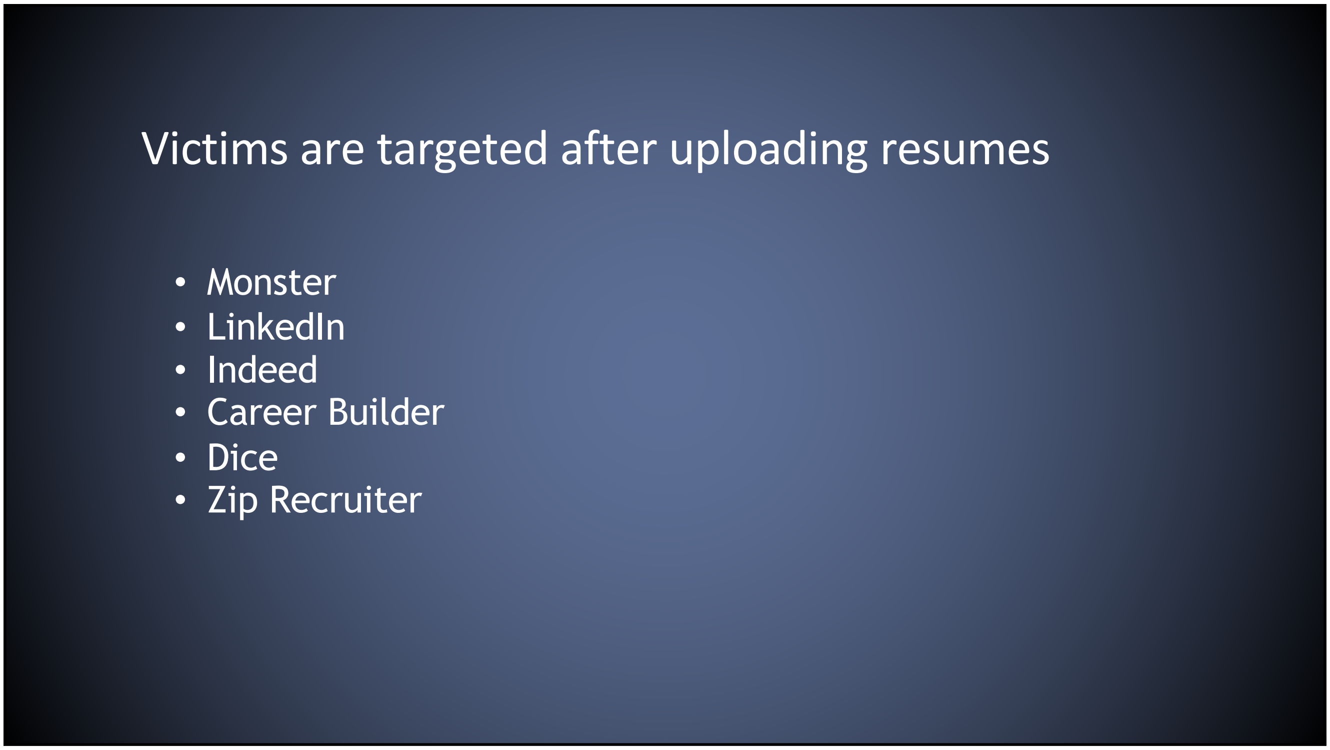
33



What’s the Connection

PO Fraud + Work From Home Scams
BEC Scams + Romance Scams

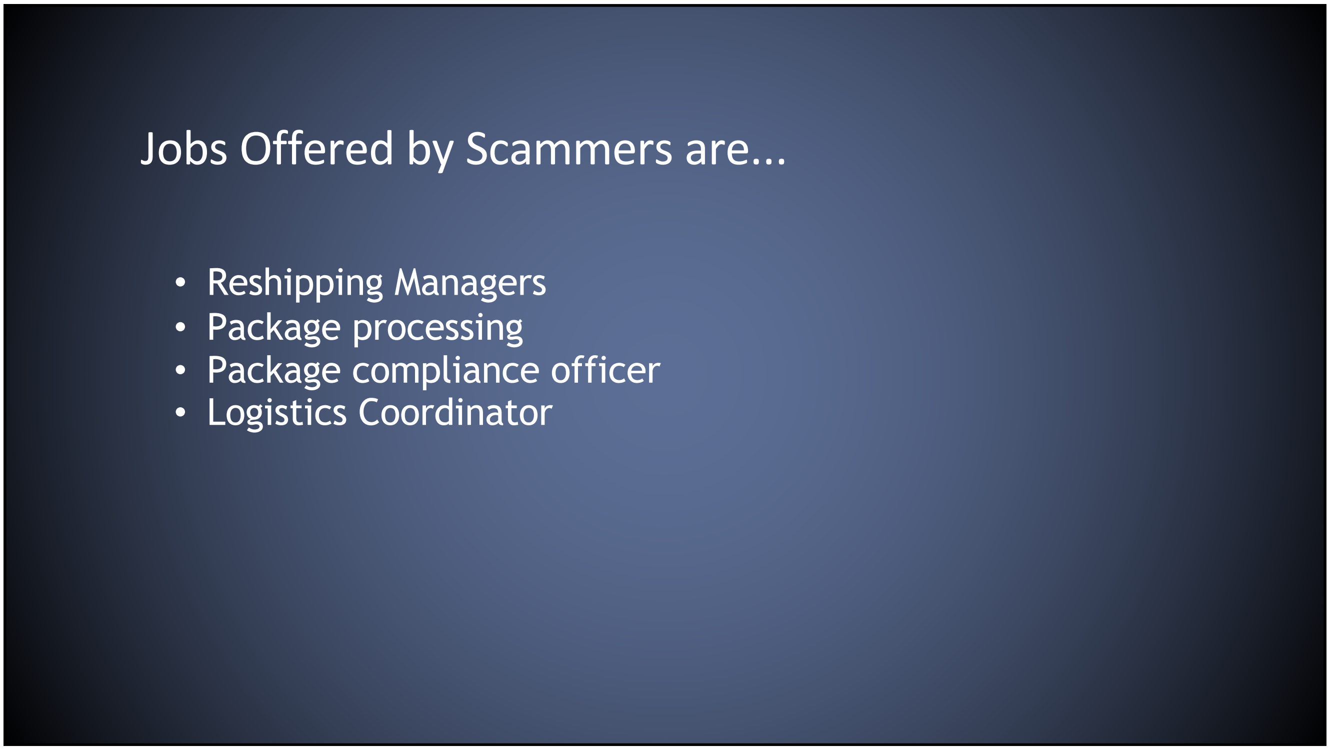
34



Victims are targeted after uploading resumes

- Monster
- LinkedIn
- Indeed
- Career Builder
- Dice
- Zip Recruiter

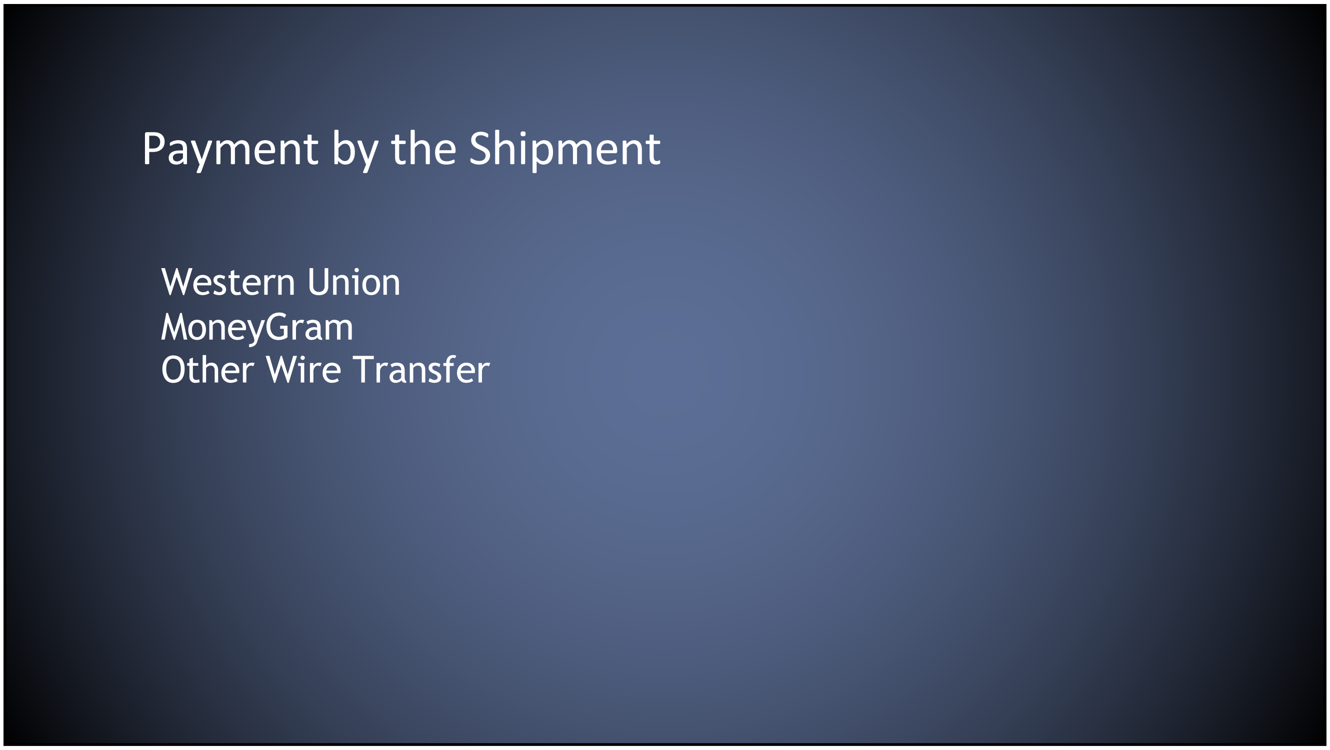
35



Jobs Offered by Scammers are…

- Reshipping Managers
- Package processing
- Package compliance officer
- Logistics Coordinator

36



Payment by the Shipment

Western Union
MoneyGram
Other Wire Transfer

37

Encouraged to...

- Find Office Space
- Find Storage Units
- Not to tell others what they do

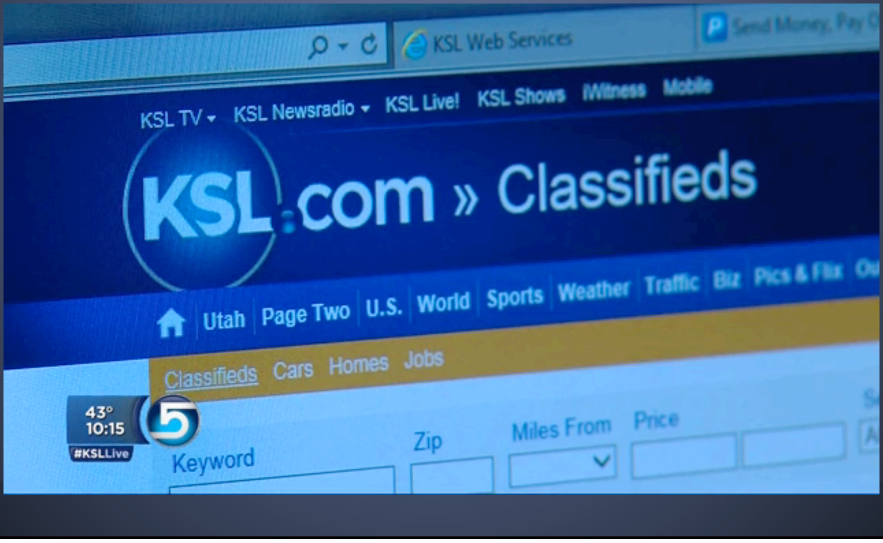
38

What can be done?

Find out where packages were sent and get them returned.
Disrupt organization by preventing shipment.
Return hundreds of thousands of dollars to local victim business.
Even make arrests in Nigeria.

39

Online Marketplace Fraud



40

Remediation and Mitigation

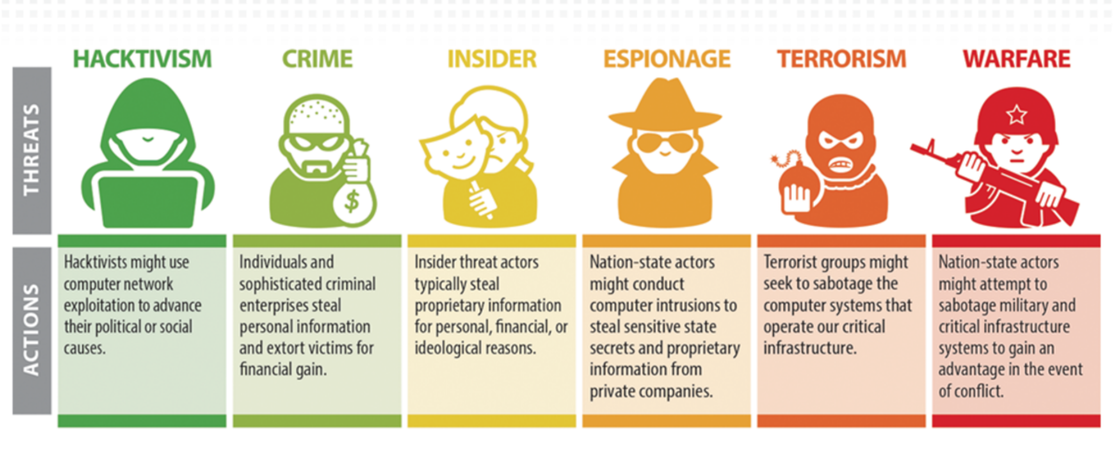
- Do not do business via text message.
- Do not click links sent by buyer. Always navigate to site by entering the address. Ebay/Paypal scams.
- Be cautious of overpayment offers.

41

Computer Intrusions

42

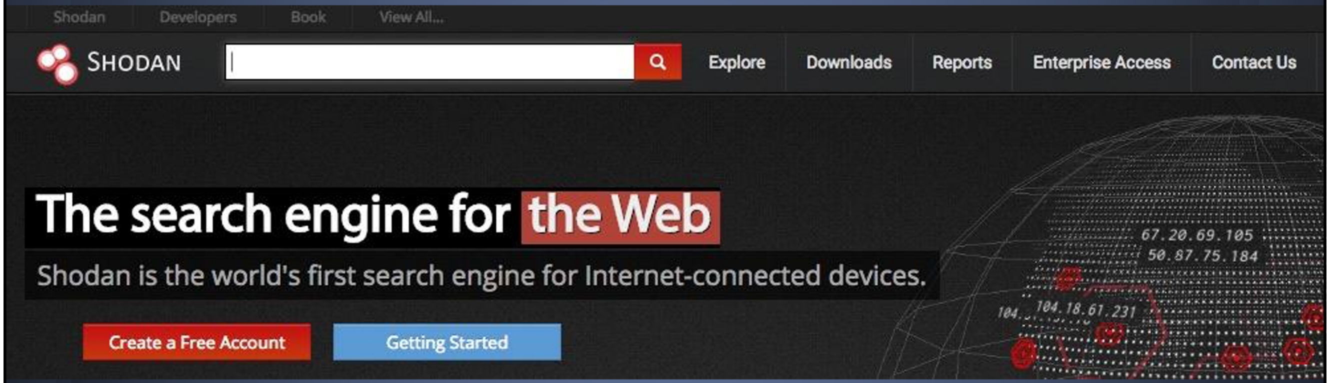
Who are the Hackers?



	HACKTIVISM	CRIME	INSIDER	ESPIONAGE	TERRORISM	WARFARE
THREATS						
ACTIONS	Hacktivists might use computer network exploitation to advance their political or social causes.	Individuals and sophisticated criminal enterprises steal personal information and extort victims for financial gain.	Insider threat actors typically steal proprietary information for personal, financial, or ideological reasons.	Nation-state actors might conduct computer intrusions to steal sensitive state secrets and proprietary information from private companies.	Terrorist groups might seek to sabotage the computer systems that operate our critical infrastructure.	Nation-state actors might attempt to sabotage military and critical infrastructure systems to gain an advantage in the event of conflict.

Computer Intrusions

- Malicious actors access and maintain control over a victim’s computer or vulnerable device.
- The attacker monitors the victim’s actions and steals sensitive information.
- Often this access was gained with a phishing email that downloaded malware which gave attacker access to computer and other accounts.



The search engine for the Web

Shodan is the world's first search engine for Internet-connected devices.

45

Payroll Intrusion

- Local Company Employees Didn’t Get Paid
- Payroll company was notified and identified DD was modified.
- Paychecks went to various bank around the nation.
- IP addresses that made changes to payroll DD info were identified
- Legal Process Served and analyzed.
- Subscriber info came back to several business. FL & AL
- Business owners interviewed.
- Windows XP computers were still being used.

46

Computer Intrusion

47

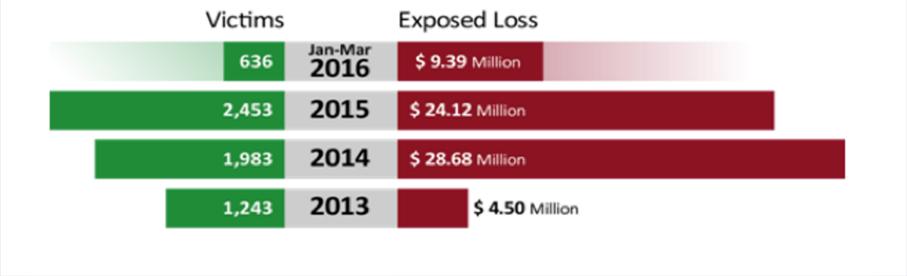
Remediation and Mitigation

- Keep firewalls turned on.
- Install and update antivirus.
- Install or update antispyware.
- Keep OS up to date.
- Turn off computer.

48

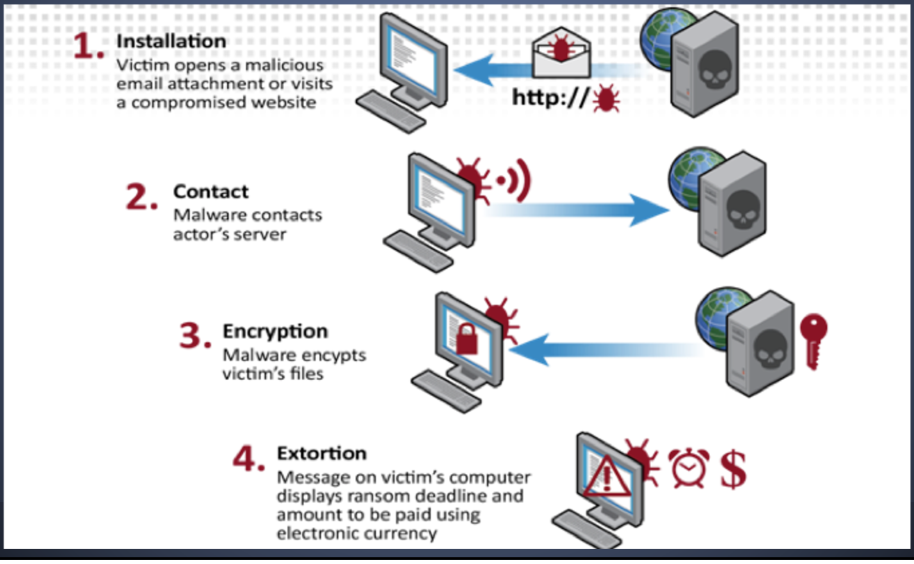
49

IC3 Data



50

Stages of Ransomware



1. Installation
Victim opens a malicious email attachment or visits a compromised website

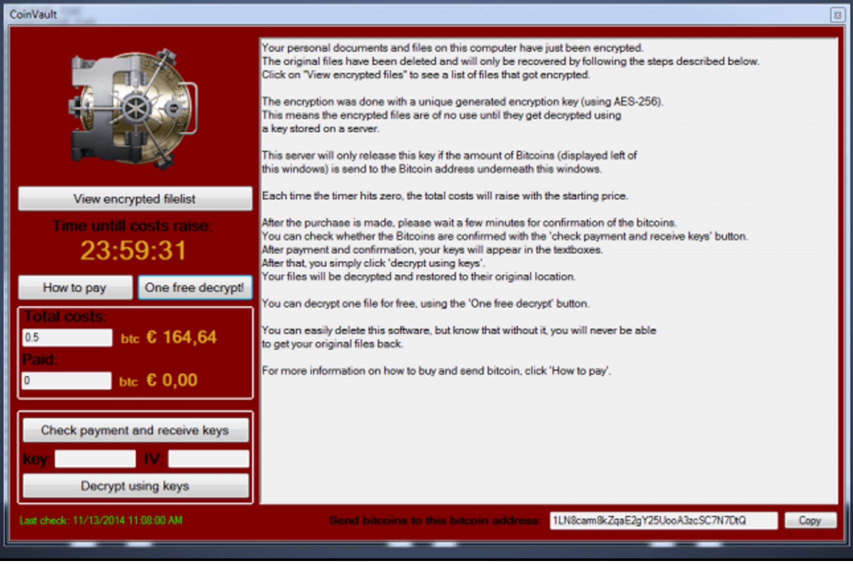
2. Contact
Malware contacts actor's server

3. Encryption
Malware encypts victim's files

4. Extortion
Message on victim's computer displays ransom deadline and amount to be paid using electronic currency

51

Ransom Page



Time untill costs raise:
23:59:31

Total costs:
0.5 btc € 164,64
Paid:
0 btc € 0,00

key: IV:

Your personal documents and files on this computer have just been encrypted.
The original files have been deleted and will only be recovered by following the steps described below.
Click on "View encrypted files" to see a list of files that got encrypted.

The encryption was done with a unique generated encryption key (using AES-256).
This means the encrypted files are of no use until they get decrypted using
a key stored on a server.

This server will only release this key if the amount of Bitcoins (displayed left of
this windows) is send to the Bitcoin address underneath this windows.

Each time the timer hits zero, the total costs will raise with the starting price.

After the purchase is made, please wait a few minutes for confirmation of the bitcoins.
You can check whether the Bitcoins are confirmed with the 'check payment and receive keys' button.
After payment and confirmation, your keys will appear in the textboxes.
After that, you simply click 'decrypt using keys'.
Your files will be decrypted and restored to their original location.

You can decrypt one file for free, using the 'One free decrypt' button.

You can easily delete this software, but know that without it, you will never be able
to get your original files back.

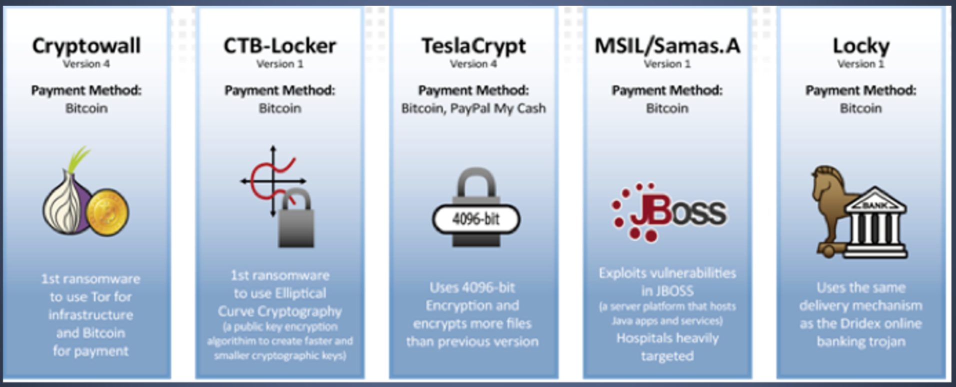
For more information on how to buy and send bitcoin, click 'How to pay'.

Last check: 11/13/2014 11:08:00 AM

Send bitcoins to this bitcoin address: 1LN8carn8kZqaE2gY25UooA3zcSC7N7DtQ

52

Ransomware Variants

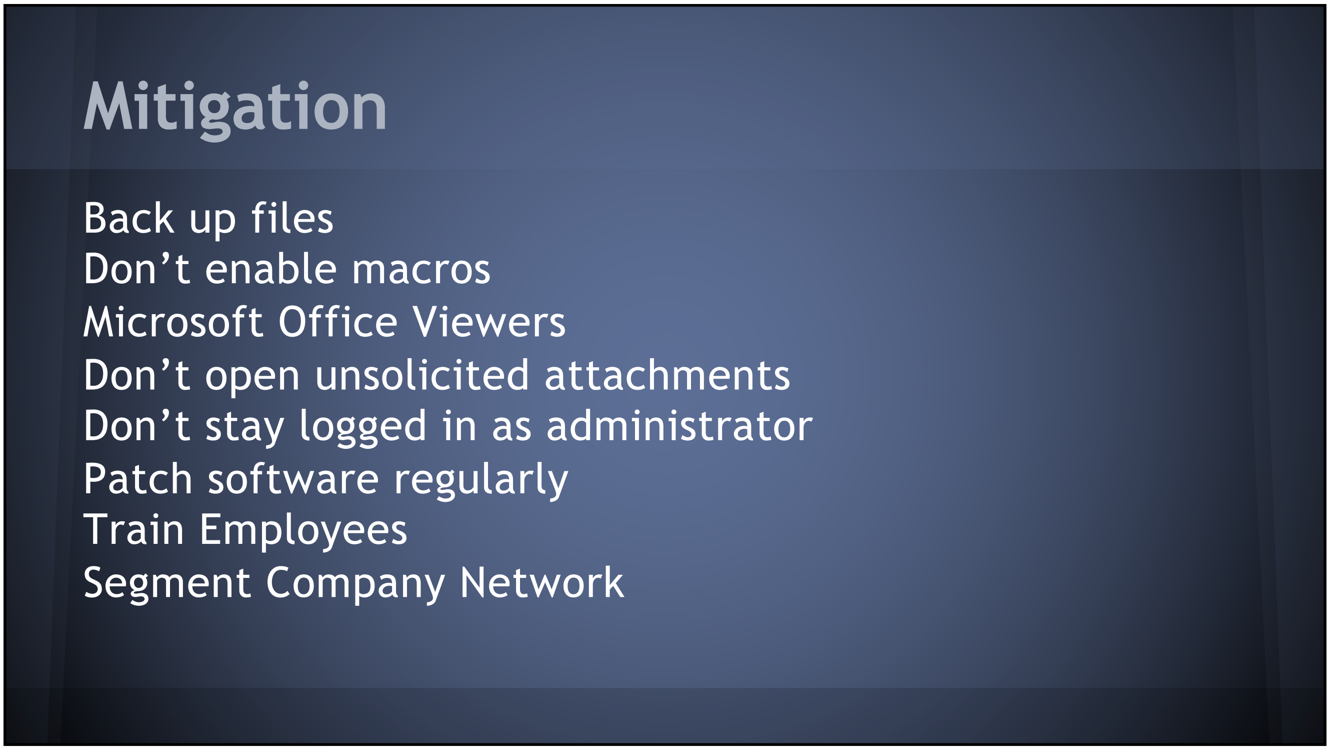


Cryptowall Version 4	CTB-Locker Version 1	TeslaCrypt Version 4	MSIL/Samas.A Version 1	Locky Version 1
Payment Method: Bitcoin	**Payment Method:** Bitcoin	**Payment Method:** Bitcoin, PayPal My Cash	**Payment Method:** Bitcoin	**Payment Method:** Bitcoin
1st ransomware to use Tor for infrastructure and Bitcoin for payment	1st ransomware to use Elliptical Curve Cryptography (a public key encryption algorithim to create faster and smaller cryptographic keys)	Uses 4096-bit Encryption and encrypts more files than previous version	Exploits vulnerabilities in JBOSS (a server platform that hosts Java apps and services) Hospitals heavily targeted	Uses the same delivery mechanism as the Dridex online banking trojan

53

Ransomware

54



Mitigation

Back up files
Don’t enable macros
Microsoft Office Viewers
Don’t open unsolicited attachments
Don’t stay logged in as administrator
Patch software regularly
Train Employees
Segment Company Network

55